

REMARKS

The present invention is a method for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol and a wireless communication apparatus for establishing a secure connection to a data communication apparatus based on a wireless application protocol, a memory card for establishing a secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol, a system for establishing a secure connection when using a wireless application protocol, a wireless communication apparatus for establishing a secure connection to a data communication apparatus through a wireless network based on a wireless application protocol and a wireless communication device for receiving therein a separate unit with memory means, the device being operable to establish a secure connection with the data communication apparatus based on a wireless application protocol through a wireless communication network. In accordance with an embodiment of the invention, the wireless communication apparatus is connected to a separate unit which contains a memory of the wireless communication apparatus. A wireless communication apparatus receives a public key and generates a master secret code. A signature may be calculated based on a chosen algorithm, the public key and the master secret code with the calculated signature being transmitted in a response to the data communication apparatus.

The data communication apparatus upon reception of the response comprising the signature calculates the master secret code based on the chosen algorithm, the signature received and the public key and establishes a secure

connection to the wireless communication device. The communication apparatus thereafter saves the master secret code on a memory means in a data communication apparatus in order to reestablish the connection at a later occasion. The use of a separate unit, such as a smart card, for re-establishing a secure connection provides a memory therein for saving the master secret code. See page 4, lines 9-15 of the specification.

The present invention stores the calculated master secret key for a period of time and utilizes it by retrieval from the memory to re-establish a connection without performing the heavy computational establishment procedure anew. See page 3, lines 16-24 of the specification and page 17, lines 29 - 30 through page 18, lines 1-6 of the specification. The invention, by storing the master secret code, eliminates the requirement to make computations for each session, which is required with the public key systems, in order to re-establish the connection between the wireless communication apparatus and the data communication apparatus.

Each of the independent claims substantively recites that the data communication apparatus utilizes the stored master secret code to re-establish the connection between the data communication apparatus and the wireless communication apparatus at a later occasion. The subject matter is not taught by the prior art relied upon by the Examiner.

The Examiner has objected to the drawings with respect to their being no description of the LCD driver 13. The Second Substitute Specification has been amended on page 11 to refer to the LCD driver 13 regarding its functional interaction between the controlled processor and controller 18 and the LCD 3.

The Second Substitute Specification has been further amended to address the Examiner's objection to the specification in Section 5 of the Office Action.

Finally, the specification stands objected to regarding antecedent basis for "memory means including a separate unit". The claims have been amended to refer in claims 1, 5, and 19 that the wireless communication apparatus "has memory means included within a separate unit". This is consistent with the teaching that the SIM card 16 as, for example, illustrated in Fig. 2, may be removed but is part of the unit when docked in the unit and provides a memory for the master secret code.

Section 7 objects to claims 5, 24 and 47 which have been amended to overcome the stated grounds of objection.

Claims 1-2, 14, 19-21, 25-40 and 45 stand rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement. The Examiner's objection is predicated upon the recitation "memory means including a separate unit" which by amendment no longer appears in claims 1, 5, and 19. Accordingly, the rejection of the claims as failing to comply with the written description requirement is overcome.

Claim 23 stands rejected under 35 U.S.C. §112, first paragraph, as failing to comply with the enablement requirement. The Examiner has construed claim 23 to be a single means claim. This ground of rejection is traversed for the following reasons.

Claim 23 recites "a memory card for establishing secure connection between a wireless communication apparatus and a data communication apparatus based on a wireless application protocol and comprising contact means for cooperation with the wireless communication apparatus comprising a memory for storing a master

secret code...". It is therefore seen that the memory card of claim 23 includes the combination of contact means and a memory and therefore, is not properly characterized as a single means claim. Accordingly, it is submitted that the rejection of claim 23 is improper and should be withdrawn.

Claims 3, 7-10, 14-18, 22, 23, 25, 27-35, 37-40, 42-44 and 46-68 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite. The claims have been amended to overcome the stated grounds of rejection. However, the Examiner's requirement regarding claim 14 is traversed. The specification teaches, on page 4, that "the present invention connects a wireless communication apparatus, for example, a cellular phone, to a separate unit, for example, a smart card, a SIM card, etc. which may store sensitive data for a secure connection". Therefore, it is seen that the specification supports the practice of the invention which is not limited to a smart card since a SIM card or other storage unit, as indicated by "etc." may be utilized. Accordingly, it is submitted that the rejection of claim 14 is improper and should be withdrawn.

Claims 1-12, 14, 19-22, 24-40 and 45 stand rejected under 35 U.S.C. §112, second paragraph, as allegedly being incomplete for omitting essential elements. The Examiner reasons that it is necessary to recite a contact means for the wireless communication apparatus as described on page 4, lines 16-20; page 19, lines 6-8; and also as recited in claims 15, 23, and 46. This ground of rejection is traversed for the following reasons.

As the Examiner is aware, 35 U.S.C. §112, second paragraph, permits the Applicant to particularly point out and distinctly claim the subject matter which the Applicant regards as the invention. With respect to the Examiner's requirement

regarding a contact means, while the specification does disclose a contact means, there is no disclosure therein indicating that the contact means is an essential part of the invention. If the Examiner persists in the stated grounds of rejection, it is requested that he point out on the record where such a teaching is found. It is submitted that the recitation of a contact means would unduly limit the present invention in the independent claims as required by the Examiner.

Claims 1, 3-12, 14-19, 21-24, 27-40, 42-44 and 46-68 stand rejected under 35 U.S.C. §103 as being unpatentable over WO 97/24831 (Ichikawa) in view of EP 0538216 (Anvret et al.). These grounds of rejection are traversed for the following reasons.

The Examiner's Response to Arguments in part states as follows:

15. Applicant's arguments filed 16 August 2004 have been fully considered but they are not persuasive.

•
•
•

Specifically, Applicant argues that none of the cited references teach a combination of a wireless communication apparatus that generates a master secret code used to initially secure connection between the wireless apparatus and a data communication apparatus, and thereafter stores the master secret code to be used at a later time. Applicant further argues that Ichikawa specifically does not disclose storing of the master secret code; however, the Examiner believes that Ichikawa does indeed teach storing of a master secret code (see page 7, line 3-page 8, line 4, as cited in the previous Office action). Applicant additionally argues that Weiss does not describe a master secret code as set forth in the claims. However, Weiss was not relied upon to teach the specific limitation of a master secret code; rather, the combination of Ichikawa and Anvret, as described in reference to the independent claims, was used to teach that limitation (see Ichikawa, page 4, lines 10-15; see also Anvret, column 6, line 28-column 7, line 13). Weiss was instead used to teach the additionally claimed limitation of Claims 2 and 20, namely storing a key only for a predetermined period of time. Applicant concedes that Weiss does teach the removal of a private key after a predetermined period of time.

The Examiner's rationale, as set forth above, and as previously argued by the Applicant, is erroneous. The Examiner has equated the master secret code, as recited substantively in each of independent claims 1, 5, 15, 19, 22, 23, 24, and 46 in different degrees of scope, as being used by the data communication apparatus to reestablish connection between the wireless communication apparatus and the data communication apparatus at a later occasion to be readable upon the use of keys. The invention's storage of the master secret code makes the use of keys and their attendant disadvantages unnecessary to reestablish connection. The prior art does not teach the storage of the claimed master secret code which provides the benefits as stated above.

The Examiner has referred to page 7, line 3, and page 8, line 4, of Ichikawa which refer to the derived key 112, which is referred to on page 8, lines 7-10, as "[t]he unique DK 112 that is generated by DEA 1 110, is dependent upon the inputs from the DEA 1 110, namely the selected series number 116 in the master key, such as 1MK shown in 506-1. These computations occur with each session. Accordingly, there is no storage and utilization of the derived key for reestablishment since each time a connection is made the derived key is required Ichikawa.

The architecture of Anvret is similar to Ichikawa in that the common key, as described in Anvret, is unique for each session as set forth in column 7, lines 8-12. Accordingly, neither Ichikawa nor Anvret have any teachings which are analogous to the claimed secret code which is used for reestablishment. Accordingly, if the proposed combination of references were made of Ichikawa and Anvret et al, the subject matter of the independent claims would not be achieved.

If the Examiner persists in the stated grounds of rejection, it is requested that he point out on the record where the prior art suggests the utilization of storage of a secret code used to provide reconnection to avoid computation overhead of calculating keys each time a connection is made which characterizes the prior art each time a session is to be established.

Claims 2, 20, 25, 26 and 45 stand rejected under 35 U.S.C. §103 as being unpatentable over Ichikawa in view of Anvret et al further in view of United States Patent 5,845,519 (Weiss). These grounds of rejection are traversed for the following reasons.

The Examiner correctly observes that Ichikawa and Anvret do not disclose saving the master key for a predetermined time. The Examiner has cited Weiss as disclosing a master key. However, as pointed out above, the utilization of keys is used for each session establishment and therefore, there is nothing analogous to Applicant's claimed storage of the master secret for reestablishing the session between the wireless communication apparatus and the data communication apparatus. Accordingly, Weiss does not cure the deficiencies noted above with respect to Ichikawa and Anvret.

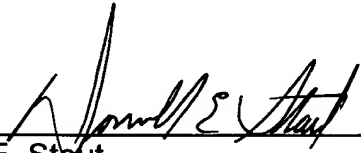
In view of the foregoing amendments and remarks, it is submitted that each of the claims in the application is in condition for allowance. Accordingly, early allowance thereof is respectfully requested.

To the extent necessary, Applicants petition for an extension of time under 37 CFR 1.136. Please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, or credit any overpayment of fees, to the

deposit account of Antonelli, Terry, Stout & Kraus, LLP, Deposit Account No.
01-2135 (1030.39437X00).

Respectfully submitted,

ANTONELLI, TERRY, STOUT & KRAUS, LLP



Donald E. Stout
Registration No. 26,422
(703) 312-6600

DES:dlh